**Usecase 2: Multiple Failed Physical Logon Attempts**

Objective: Detect and create an alert when physical brute force logon attempts occur

Log Source: Windows Security Event Logs

Event ID: 4625- “an account failed to log on”

Example Target Log From Event Viewer:

An account failed to log on.

Subject:

Security ID: SYSTEM

Account Name: <system name>

Account Domain: WORKGROUP

Logon ID: 0x3E7

Logon Type: 2

Account For Which Logon Failed:

Security ID: NULL SID

Account Name: -

Account Domain: -

Failure Information:

Failure Reason: An Error occured during Logon.

Status: 0xC000006D

Sub Status: 0xC0000380

Process Information:

Caller Process ID: 0xbd4

Caller Process Name: C:\Windows\System32\svchost.exe

Network Information:

Workstation Name: -

Source Network Address: 127.0.0.1

Source Port: 0

Detailed Authentication Information:

Logon Process: User32

Authentication Package: Negotiate

Transited Services: -

Package Name (NTLM only): -

Key Length: 0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

Logon type 2 refers to physical, keyboard logon attempts

Pre-configuration: N/A

Custom Wazuh Rule:

A screen shot of a computer code

AI-generated content may be incorrect.

Frequency 4+timeframe 300 means there must be 4 attempts within 5 minutes for the alert to trigger

If\_matched\_sid is used for custom rules with frequency/time requirements, the specific if\_sid is 60122: Logon failure with incorrect details, seen below:

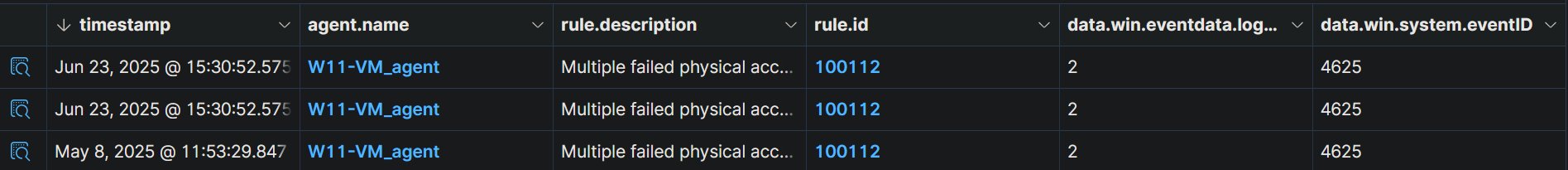
A computer screen shot of a black background

AI-generated content may be incorrect.

win.system.eventID=^4625$ filters for 60122 logs that have the exact match of ID 4625

win.eventdata.logonType=^2$ further filters these logs for events that have logon Typw 2

Example Alerts:



Verification of fields:

A screenshot of a computer

AI-generated content may be incorrect.